



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/637,431

08/08/2003

Anil Singhal

09851.0006-00000

2626

22852

7590

05/20/2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP

901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

KIM, JUNG W

ART UNIT

PAPER NUMBER

2132

MAIL DATE

DELIVERY MODE

05/20/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/637,431	Applicant(s) SINGHAL ET AL.	
	Examiner JUNG KIM	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 February 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29,32-34 and 40-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29,32-34 and 40-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office action is in response to the RCE filed on 2/6/08.
2. Claims 1-25, 21-29, 32-34 and 40-43 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/6/08 has been entered.

Response to Amendment

4. The amendment to the Specification and the claims, i.e. the elimination of a carrier wave as a program storage medium, overcomes the 101 rejection to claims 40-43.
5. The Declarations ("Declaration A" and "Declaration B") filed on 2/6/08 under 37 CFR 1.131 are sufficient to overcome the Day reference. However, upon further search and consideration, the claims are rejected under 35 USC 103(a) as being unpatentable over Vairavan in view of Esbensen (see below).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-7, 12-15, 21-28, 34 and 40-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan US Patent Application Publication No. 20020083344 (hereinafter Vairavan) in view of Esbensen US 5,796,942 (hereinafter Esbensen).

8. As per claims 1-3, Vairavan discloses a method of intrusion detection, comprising:

- a. receiving at a probe data packets communicating over a first network link; converting the received data packets into a format suitable for a second network link; wherein the first network link is a WAN link and the second network link is a LAN and data packets are communicated over a third network link; (paragraph 0047: network device has an access interface that couples one or more WANs and one or more LANs)
- b. and monitoring, by the probe, the received packets to evaluate network performance. (paragraph 0090)

9. Vairavan does not disclose transmitting, by the probe, over a second network link, the packets to an intrusion detection system in communication with the second network link. Esbensen discloses an intrusion detection system whereby an

agent/handler captures packets and transmits the packets over a second network link to an intrusion detection system in communication with the second network link. (Abstract; fig. 1; fig. 4). This setup has the advantage of maintaining a dedicated intrusion detection system without decreasing network performance. (Esbensen, 2:42-47)

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method of Vairavan to transmit, by the probe over a second network link, the packets to an intrusion detection system in communication with the second network link. One would be motivated to do so to accrue the benefits of a dedicated intrusion detection system as taught by Esbensen. The aforementioned cover the limitations of claims 1-3.

10. As per claim 4, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. In addition, Vairavan further discloses the step of aggregating the data packets received over the first network and the data packets received over the third network. (fig. 1, ports 115(a-g) and interface 120, 125 and 130)

11. As per claims 5-7, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. In addition, Vairavan further discloses the first network link operates using at least one of HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol; wherein the first network link comprises a

Art Unit: 2132

protocol that encapsulates data traffic; wherein the protocol comprises at least one of MPLS protocol, GMPLS protocol, VLAN (802.1q) protocol, HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol. (paragraph 0047)

12. As per claims 12 and 13, the rejections of claims 8-10 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. In addition, Vairavan further discloses the converting step comprises: storing received packets in a collection buffer; stripping header information associated with a protocol of the first network link; and adding header information associated with a protocol of the second network link; wherein the step of storing comprises storing packets received from at least one of the first network and the third network link. (Fig. 1: inherent in a protocol conversion from WAN to LAN)

13. As per claim 14, the rejections of claims 12 and 13 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. In addition, the stripping step further comprising stripping header and checksum information associated with the protocol of the first network link and the adding step further comprising adding header and checksum information associated with the protocol of the second network link; wherein the step of storing comprises storing packets received from at least one of the first network link and a third network link are obvious enhancements because different communication protocols utilized different checksum values.

14. As per claim 15, the rejections of claims 12 and 13 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. In addition, the step of stripping comprising stripping at least one of a Layer 2 MAC header, an Ethernet source address, and an Ethernet destination address is an obvious enhancement because Ethernet is conventionally utilized in LAN technology.

15. As per claims 21-28 and 34, the rejections of claims 1-15 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. In addition, Vairavan and Esbensen disclose the first network link comprises a protocol that encapsulates data traffic (WAN link). The aforementioned cover the limitations of claims 21-28 and 34.

16. As per claims 40-43, they are claims corresponding to claims 1-7, 12-15, 21-28 and 34, and they do not teach or define above the information claimed in claims 1-7, 12-15, 21-28 and 34. Therefore, claims 40-43 are rejected as being unpatentable over Vairavan in view of Esbensen for the same reasons set forth in the rejections of claims 1-7, 12-15, 21-28 and 34.

17. Claims 8-11, 29, 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan in view of Esbensen and further in view of Schneier et al. US 7,159,237 (hereinafter Schneier)

Art Unit: 2132

18. As per claims 8-11, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Esbensen are incorporated herein. Neither Vairavan nor Esbensen disclose the step of maintaining, by the probe, an audit trail buffer for forensic analysis; wherein the audit trail buffer comprises a memory for recording monitored packets; wherein the memory records packets from at least one of the first network link and the third network link; upon receiving, by the probe, an event notification, communicating, by the probe, the current contents of the audit trail buffer. Schneier discloses a method for monitoring packet flows via probes/sentries, whereby data sensors collect data, filtering subsystems filter the data and an Anomaly engine analyzes the data; Anomaly engine determines noteworthy information that may be worthy of further analysis and forwards such information to a communications and resource coordinator; whereby the coordinator forwards the information to the intrusion detection system. (col. 8:35-63) Such a feature enables uninteresting information to be discarded at the probe before being analyzed by a central intrusion detection system, thereby reducing the amount of information to be processed by the central intrusion detection system. (8:45-47) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Vairavan to further include the steps of maintaining, by the probe, an audit trail buffer for forensic analysis; wherein the audit trail buffer comprises a memory for recording monitored packets; wherein the memory records packets from at least one of the first network link and the third network link; upon receiving, by the probe, an event notification, communicating, by the probe, the current contents of the audit trail buffer. One would be motivated to do so to reduce the amount

of information to be processed by the central intrusion detection system as known to one of ordinary skill in the art.

19. As per claims 29, 32 and 33, they are claims corresponding to claims 8-11, and they do not teach or define above the information claimed in claims 8-11. Therefore, claims 29, 32 and 33 are rejected as being unpatentable over Vairavan in view of Esbensen and Schneier for the same reasons set forth in the rejections of claims 8-11.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See enclosed PTO-892.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner AU 2132